

A Scalable Semantics-Based Verification System for Flight Critical Software, Phase I

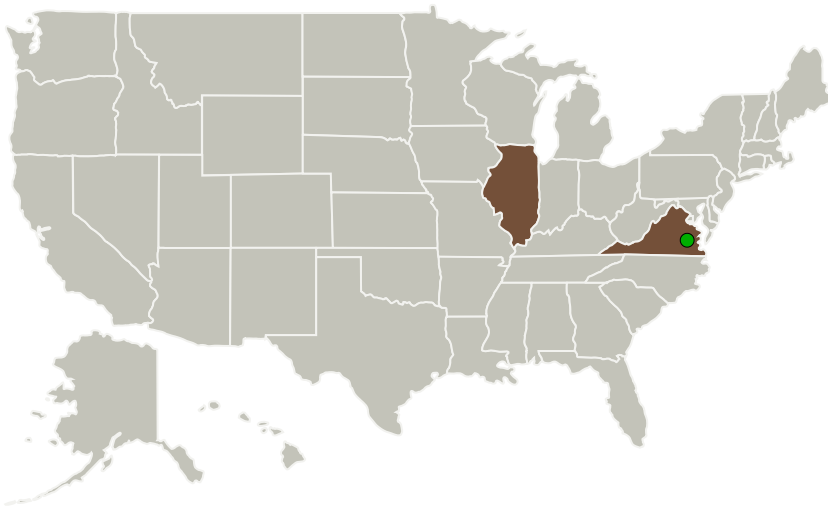
Completed Technology Project (2013 - 2013)



Project Introduction

Modern flight-critical systems include hundreds of thousands to millions of lines of code. The Boeing 777, for instance, includes over 2 million lines of code. Future projects will only feature an increasing amount of source code, mostly written in the C programming language. The only way to completely ensure the safety of flight critical systems is through static, formal program verification. In order to effectively verify such large programs written in the C programming language, we propose a scalable system for the verification of program written in C based on matching logic, or program verification logic. Matching logic has the benefit of being more scaleable than traditional Hoare/seperation logic verifiers because they build a large first order logic proof goal for entire functions at a time, while matching logic proceeds in program order, proving goals incrementally. Additionally, matching logic verifiers are based on operational semantics of the programming language in question. Operational semantics offer the benefit of being fully executable, so that one may increase belief that they are correct by testing typical compiler test suite programs, such as the GCC torture tests for the C language. Ultimately, our proposed research will result in a verifier that is both more scalable and more trustworthy than the competition.

Primary U.S. Work Locations and Key Partners



A Scalable Semantics-Based Verification System for Flight Critical Software

Table of Contents

Project Introduction	1
Primary U.S. Work Locations and Key Partners	1
Project Transitions	2
Images	2
Organizational Responsibility	2
Project Management	2
Technology Maturity (TRL)	3
Technology Areas	3
Target Destinations	3

A Scalable Semantics-Based Verification System for Flight Critical Software, Phase I


Completed Technology Project (2013 - 2013)



Organizations Performing Work	Role	Type	Location
Runtime Verification Inc	Lead Organization	Industry	Champaign, Illinois
● Langley Research Center(LaRC)	Supporting Organization	NASA Center	Hampton, Virginia

Primary U.S. Work Locations	
Illinois	Virginia

Project Transitions

 **May 2013:** Project Start

 **November 2013:** Closed out

Closeout Documentation:

- Final Summary Chart(<https://techport.nasa.gov/file/140358>)

Images



Project Image

A Scalable Semantics-Based Verification System for Flight Critical Software

(<https://techport.nasa.gov/image/126330>)

Organizational Responsibility

Responsible Mission Directorate:

Space Technology Mission Directorate (STMD)

Lead Organization:

Runtime Verification Inc

Responsible Program:

Small Business Innovation Research/Small Business Tech Transfer

Project Management

Program Director:

Jason L Kessler

Program Manager:

Carlos Torrez

Principal Investigator:

Patrick Meredith

Co-Investigator:

Patrick Meredith

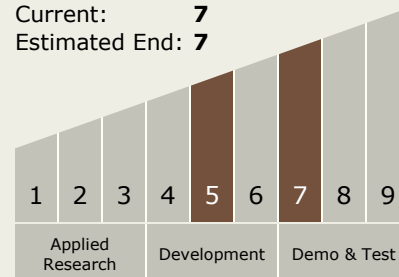
A Scalable Semantics-Based Verification System for Flight Critical Software, Phase I

Completed Technology Project (2013 - 2013)



Technology Maturity (TRL)

Start: 5
Current: 7
Estimated End: 7



Technology Areas

Primary:

- TX11 Software, Modeling, Simulation, and Information Processing
 - └ TX11.2 Modeling
 - └ TX11.2.1 Software Modeling and Model Checking

Target Destinations

The Moon, Mars, Outside the Solar System, The Sun, Earth, Others Inside the Solar System